OIPE IAP52
JUL 27 2006
PATENT & TRADEMARK OFFICE

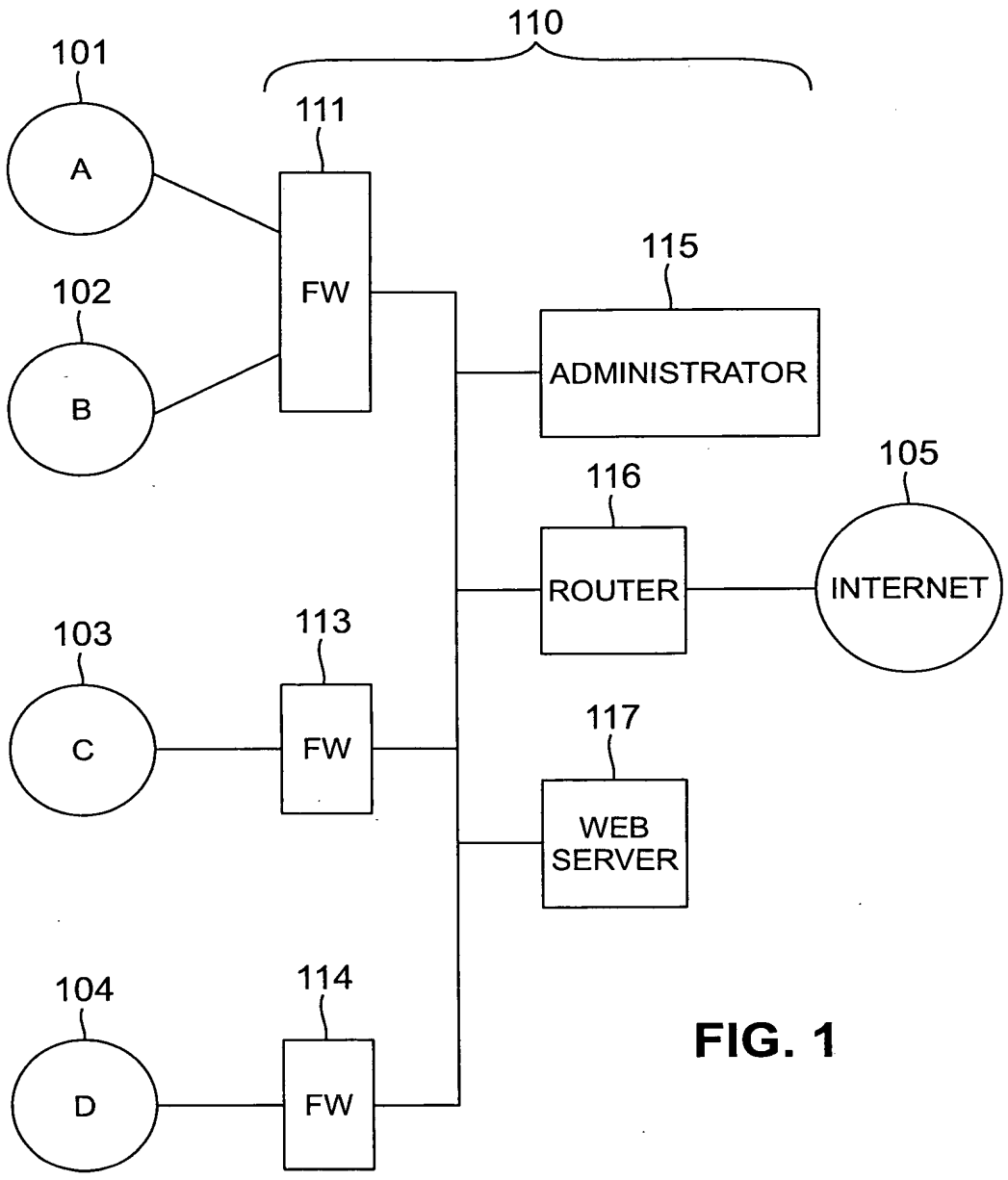

FIG. 1

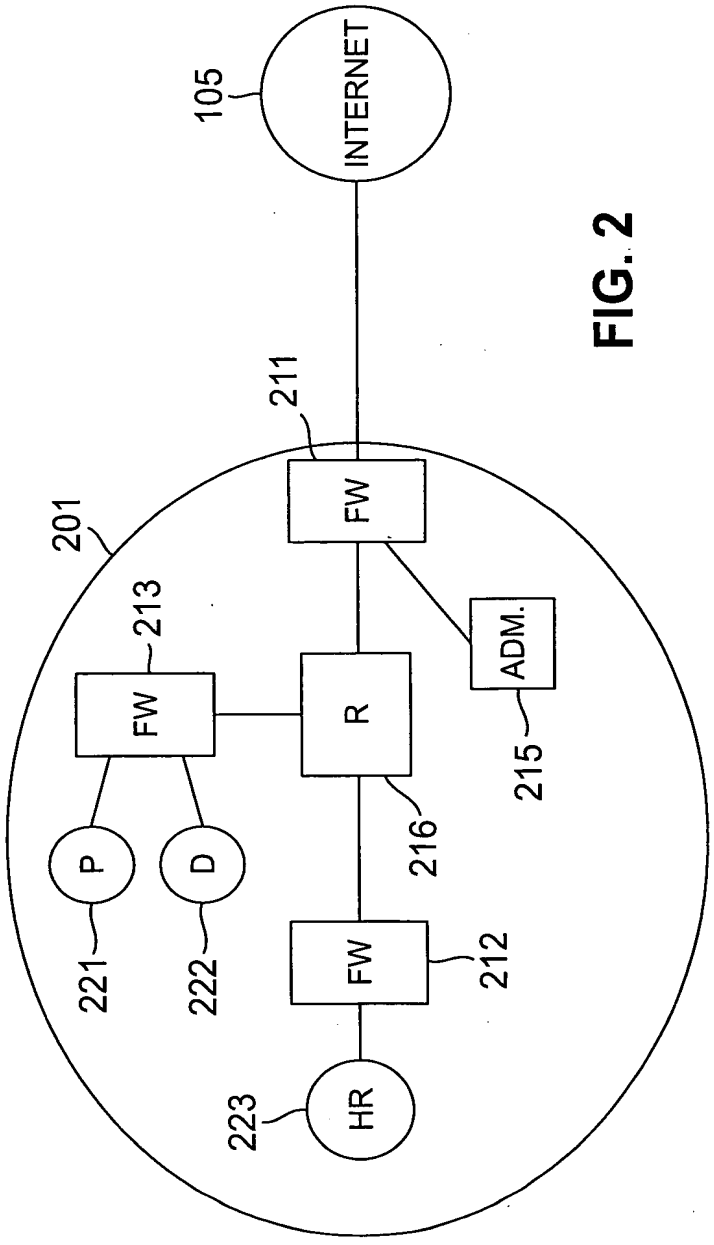
105
INTERNET
211
FW
201
213
FW
R
ADM.
215
216
P
D
221
222
FW
212
223
HR

FIG. 2

RULE NO.	SOURCE HOST	DEST. HOST	SERVICE	ACTION
10	A	B	FTP	PASS
20	A	*	*	DROP
30	B	C	TELNET	PROXY
40	*	D	MAIL	PASS

FIG. 3

SESSION KEY	HARDWARE ADDRESS	INTERFACE	RULE NO.	ALARM CODE	STAT. INFO.	ACTION
A, B, TELNET	Ma, Mb	en0, en1	10	10	5 PKTS.	PASS
B, A, TELNET	Mb, Ma	en1, en0	10	10	5 PKTS.	PASS
C, A, MAIL	Mc, Ma	en1, en0	30	20	100 PKTS.	PASS
A, C, MAIL	Ma, Mc	en0, en1	30	20	10 PKTS.	PASS
D, A, TELNET	Md, Ma	en1, en0	40	30	15 PKTS.	DROP
E, A, MAIL	Me, Ma	en1, en0	30	10	30 PKTS.	PASS
A, E, MAIL	Ma, Me	en0, en1	30	10	10 PKTS.	PASS

FIG. 4

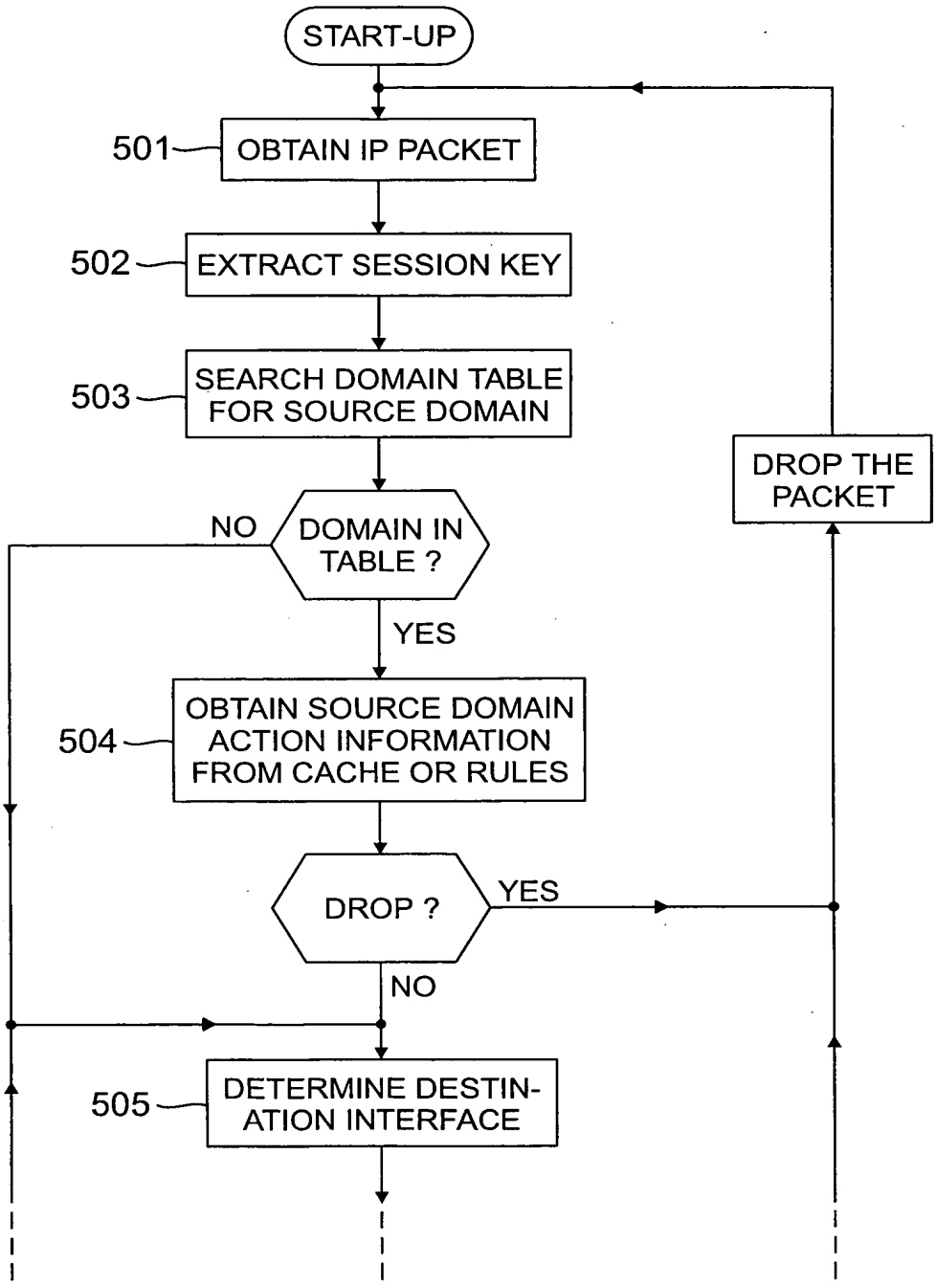
START-UP
501
OBTAIN IP PACKET
502
EXTRACT SESSION KEY
503
SEARCH DOMAIN TABLE FOR SOURCE DOMAIN
NO
DOMAIN IN TABLE ?
YES
DROP THE PACKET
504
OBTAIN SOURCE DOMAIN ACTION INFORMATION FROM CACHE OR RULES
DROP ?
YES
NO
505
DETERMINE DESTIN-ATION INTERFACE

FIG. 5A

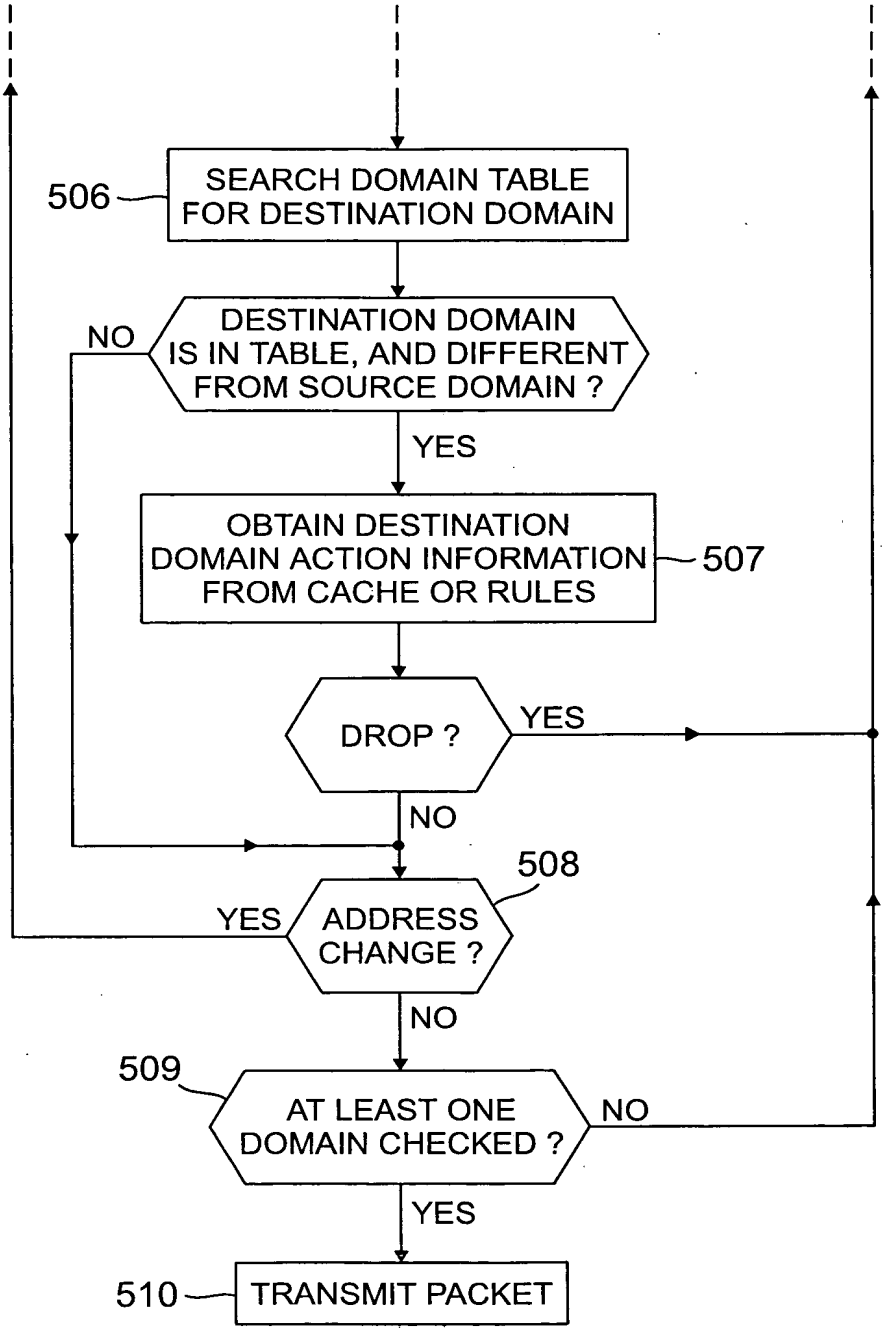
506
SEARCH DOMAIN TABLE FOR DESTINATION DOMAIN
NO
DESTINATION DOMAIN IS IN TABLE, AND DIFFERENT FROM SOURCE DOMAIN ?
YES
OBTAIN DESTINATION DOMAIN ACTION INFORMATION FROM CACHE OR RULES
507
DROP ?
YES
NO
508
YES
ADDRESS CHANGE ?
NO
509
AT LEAST ONE DOMAIN CHECKED ?
NO
YES
510
TRANSMIT PACKET

FIG. 5B

INTERFACE	ADDRESS RANGE	DOMAIN
0	10.50.0.0 - 10.50.255.255	A
0	10.60.0.0 - 10.60.255.255	B
1	*	C
2	*	*

FIG. 6

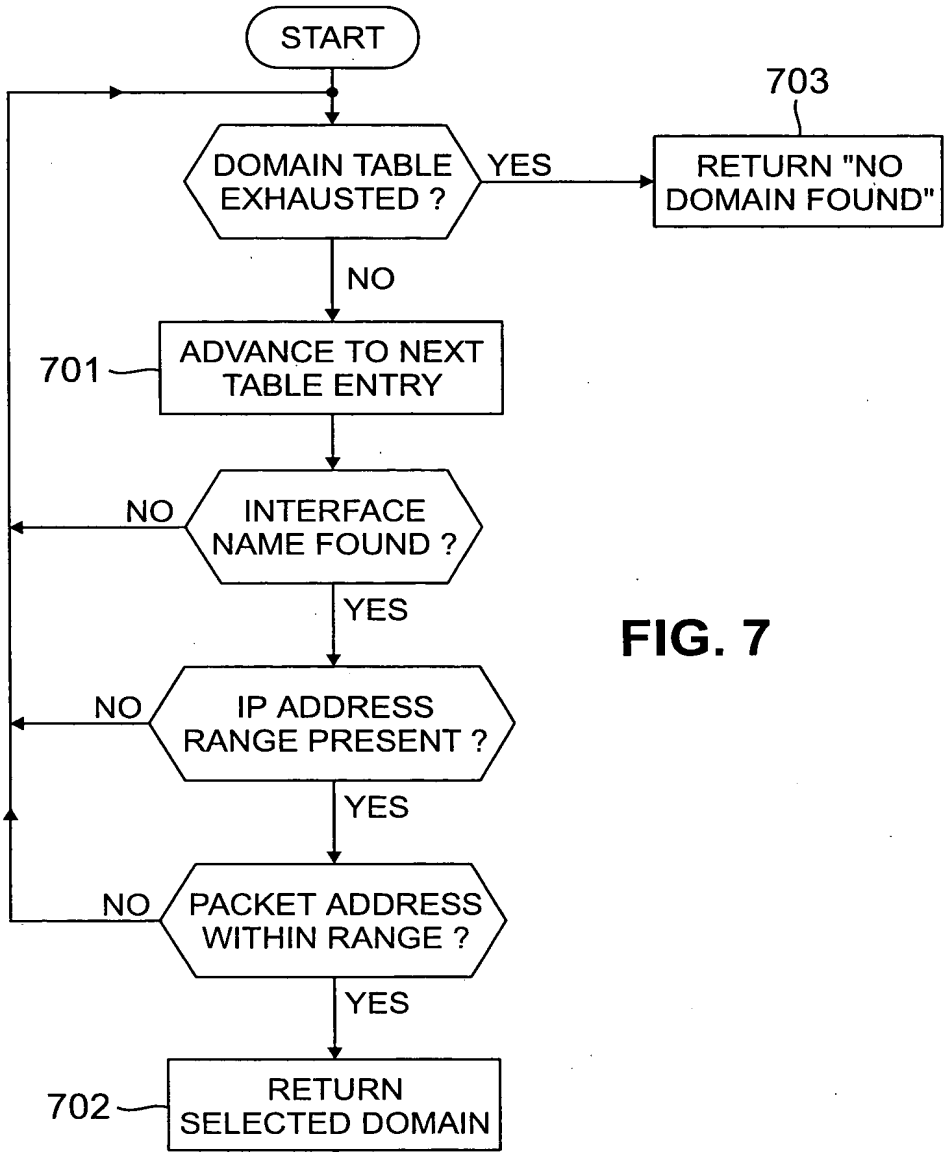
START
703
DOMAIN TABLE EXHAUSTED ?
YES
RETURN "NO DOMAIN FOUND"
NO
701
ADVANCE TO NEXT TABLE ENTRY
NO
INTERFACE NAME FOUND ?
YES
NO
IP ADDRESS RANGE PRESENT ?
YES
NO
PACKET ADDRESS WITHIN RANGE ?
YES
702
RETURN SELECTED DOMAIN

FIG. 7

NAME	SOURCE HOST	DEST. HOST	SERVICE	ACTION	HIT COUNT
TRACEROUTE	^	*	TRACEROUTE	PASS	1
PPTP	•	•	TCP/1723	PASS	1
TELNET	A	B	TELNET	DROP	10
REALAUDIO	^	*	TCP/7070	PASS	1

FIG. 8

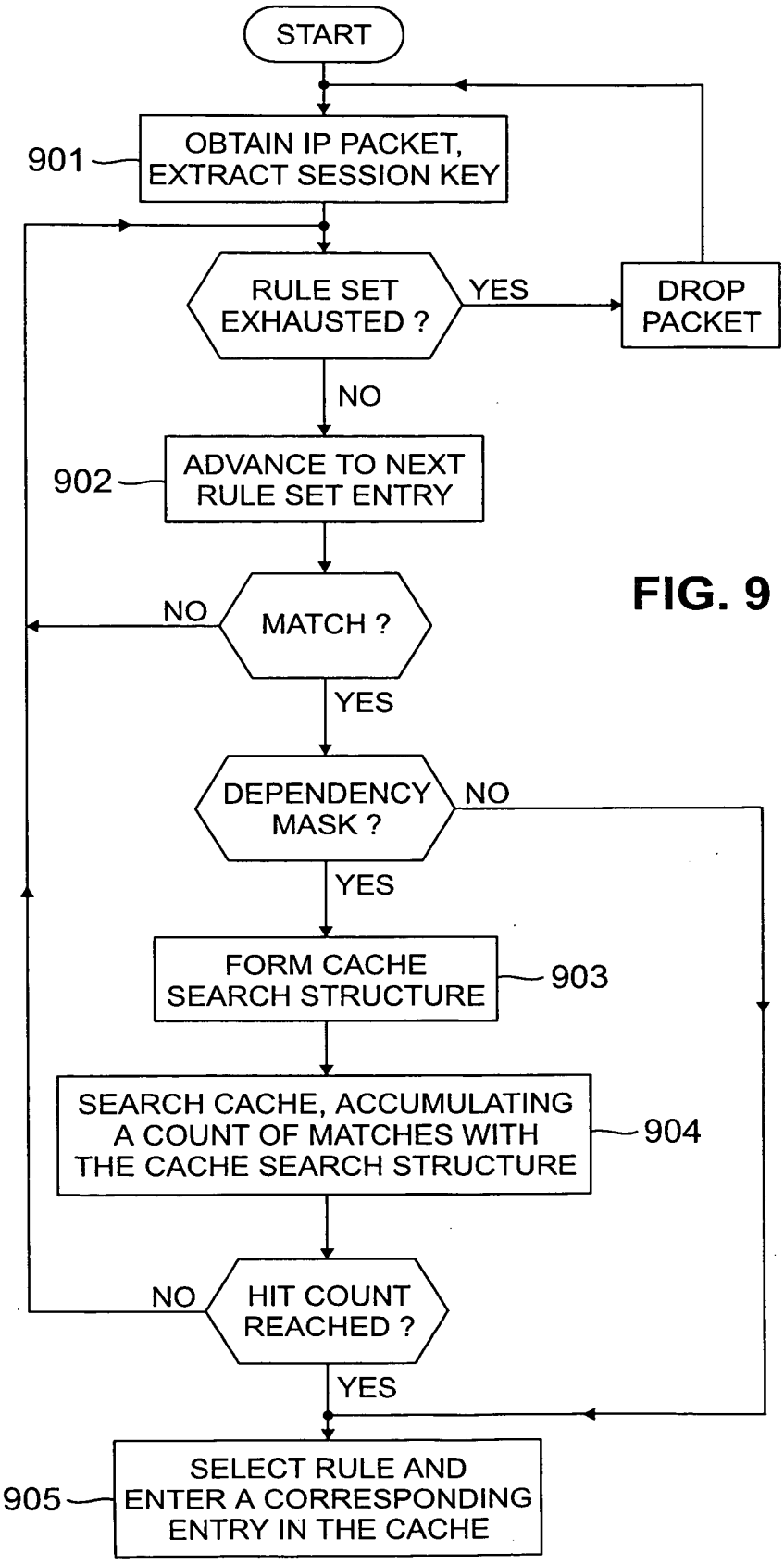
START
OBTAIN IP PACKET, EXTRACT SESSION KEY
901
RULE SET EXHAUSTED ?
YES
DROP PACKET
NO
ADVANCE TO NEXT RULE SET ENTRY
902
NO
MATCH ?
YES
DEPENDENCY MASK ?
NO
YES
FORM CACHE SEARCH STRUCTURE
903
SEARCH CACHE, ACCUMULATING A COUNT OF MATCHES WITH THE CACHE SEARCH STRUCTURE
904
NO
HIT COUNT REACHED ?
YES
SELECT RULE AND ENTER A CORRESPONDING ENTRY IN THE CACHE
905

FIG. 9

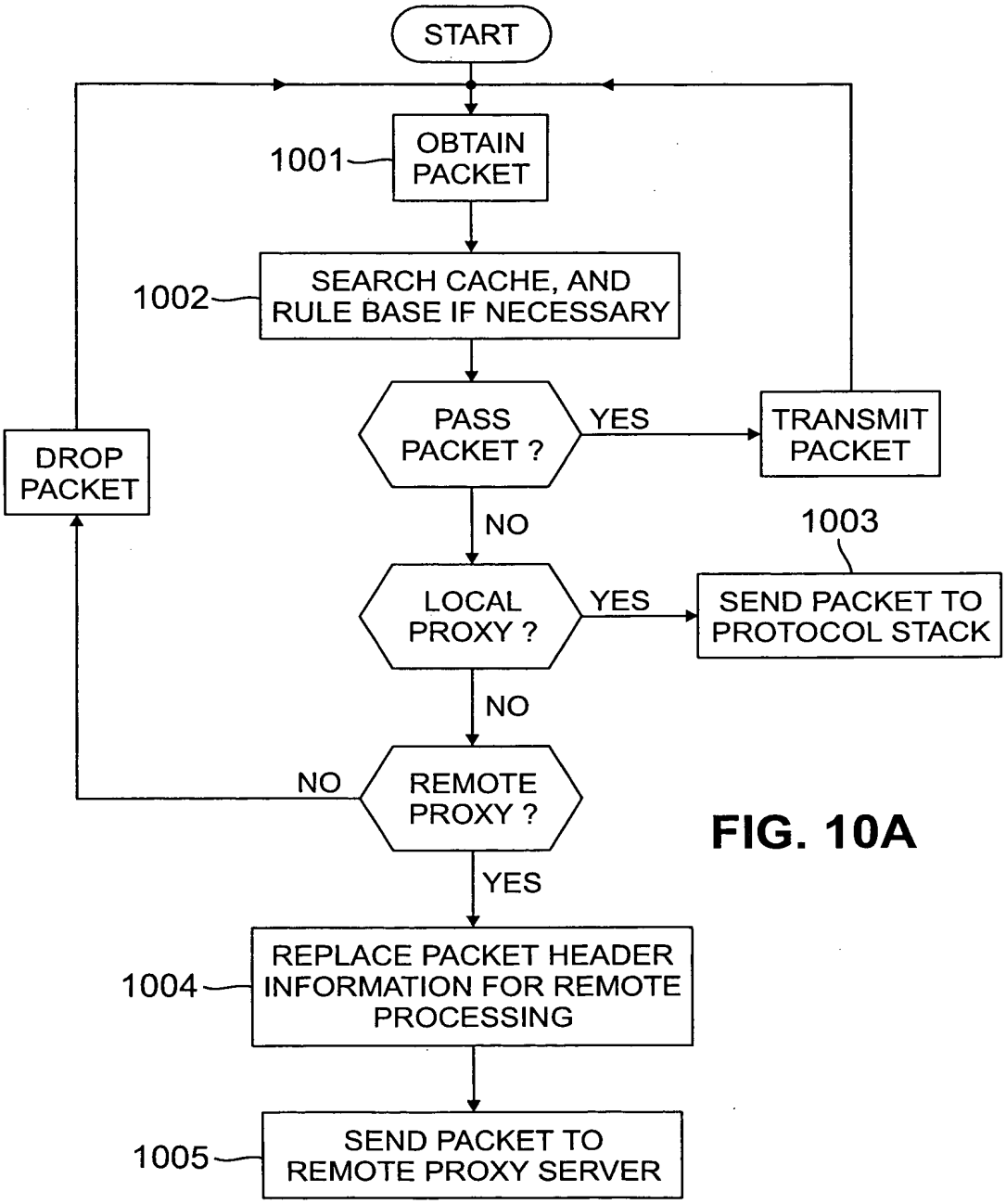
START
1001
OBTAIN PACKET
1002
SEARCH CACHE, AND RULE BASE IF NECESSARY
PASS PACKET ?
YES
TRANSMIT PACKET
DROP PACKET
NO
1003
LOCAL PROXY ?
YES
SEND PACKET TO PROTOCOL STACK
NO
NO
REMOTE PROXY ?
YES
1004
REPLACE PACKET HEADER INFORMATION FOR REMOTE PROCESSING
1005
SEND PACKET TO REMOTE PROXY SERVER

FIG. 10A

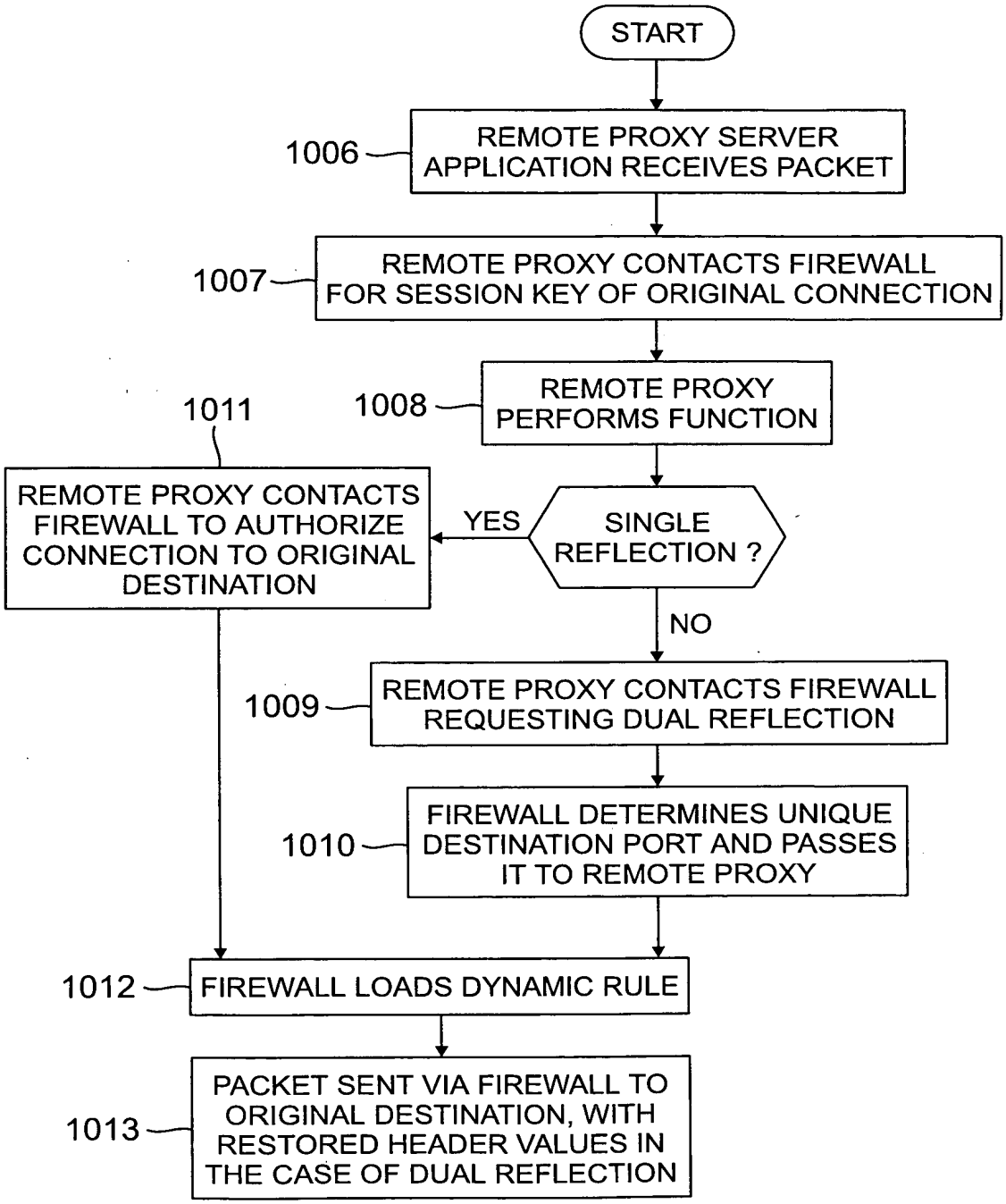
START
1006
REMOTE PROXY SERVER APPLICATION RECEIVES PACKET
1007
REMOTE PROXY CONTACTS FIREWALL FOR SESSION KEY OF ORIGINAL CONNECTION
1008
REMOTE PROXY PERFORMS FUNCTION
1011
SINGLE REFLECTION ?
YES
REMOTE PROXY CONTACTS FIREWALL TO AUTHORIZE CONNECTION TO ORIGINAL DESTINATION
NO
1009
REMOTE PROXY CONTACTS FIREWALL REQUESTING DUAL REFLECTION
1010
FIREWALL DETERMINES UNIQUE DESTINATION PORT AND PASSES IT TO REMOTE PROXY
1012
FIREWALL LOADS DYNAMIC RULE
1013
PACKET SENT VIA FIREWALL TO ORIGINAL DESTINATION, WITH RESTORED HEADER VALUES IN THE CASE OF DUAL REFLECTION

FIG. 10B